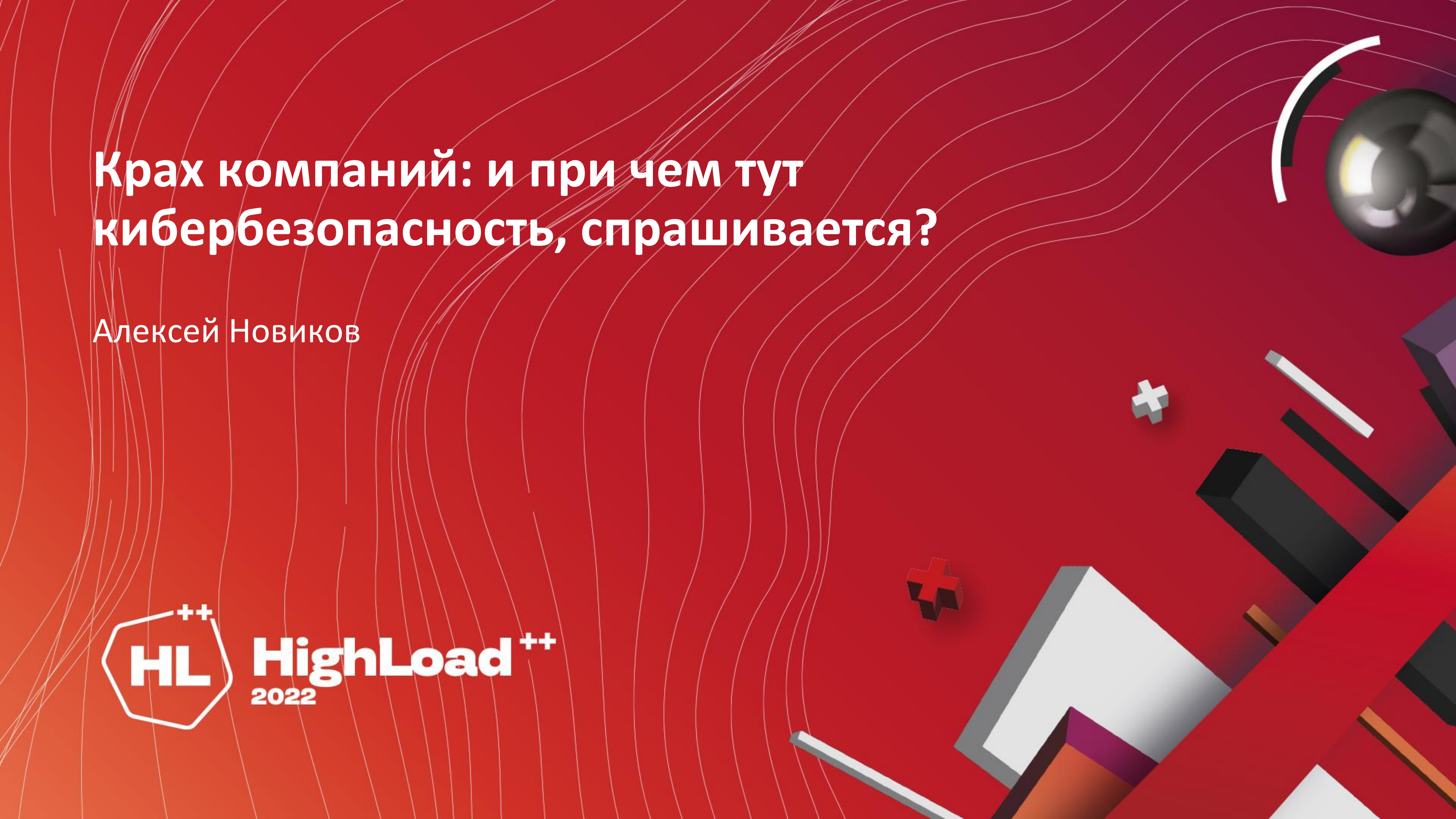

Крах компаний: и при чем тут кибербезопасность, спрашивается?
Алексей Новиков
HL
HighLoad++
2022






# Алексей
# Новиков

**Директор экспертного центра безопасности**
**Positive Technologies**
**(PT Expert Security Center)**



# Инцидентов становится только больше




| | 2022 | 2021 |
|---|---|---|
| Q1 | 714 | 607 |
| Q2 | 702 | 609 |
| Q3 | | 580 |
| Q4 | | 620 |





# Последствия




| Последствие | Организации |
|---|---|
| Нарушение основной деятельности | 50% |
| Утечка конфиденциальной информации | 40% |
| Ущерб интересам государства | 18% |
| Прямые финансовые потери | 12% |
| Использование ресурсов для проведения атак | 7% |
| Другое | 4% |
| Неизвестно | 16% |

0% 5% 10% 15% 20% 25% 30% 35% 40% 45% 50% 55%

Организации





# Целью являются все!




18%
13%
7%
7%
6%
5%
4%
4%
18%
18%

- Госучреждения
- Промышленность
- Наука и образование
- Медицинские учреждения
- Транспорт
- IT-компании
- Сфера услуг
- Блокчейн-проекты
- Другие
- Без привязки к отрасли





# Восстановление растягивается на годы




<10%

**от общих последствий** приходится на усилия по разбору инцидента*

Разбор инцидента

Управление последствиями

Восстановление бизнеса

Год 1 2 3 4 5

!

Хронология инцидента

Обнаружение инцидента

**Несколько дней или недель**

- Остановить компрометацию
- Устранить уязвимости и усилить меры безопасности
- Проинформировать клиентов, партнеров и другие сторонние организации
- Восстановить работоспособность бизнеса

**Несколько недель или месяцев**

- Создать временную инфраструктуру или наладить временные процессы
- Подключить юристов
- Решить вопросы с аудитами и соблюдением законодательства
- Урегулировать отношения с клиентами, партнерами и другими сторонами

**Несколько месяцев или лет**

- Компенсировать ущерб, причиненный бизнесу
- Реорганизовать процессы и активы
- Инвестировать в программы кибербезопасности, чтобы стать сильнее

*https://www2.deloitte.com/gr/en/pages/risk/articles/beneath-the-surface-of-a-cyberattack.html

# - 35% от стоимости акций




Published on TradingView.com, November 20, 2022 23:06:37 MSK
**EFX, 1D O:**200.00 **H:**202.49 **L:**198.73 **C:**200.04

**Equifax Inc.**

**EFX, 1Д, NYSE**
Volume

150.00
140.00
130.00
120.00
115.06
110.00
100.00
90.00

ай Июн Июл Авг Сен Окт Ноя Дек **2018** Фев

TradingView



# Equifax Inc




Что: утечка 145 млн персональных данных, 209 тысяч кредитных карт

Где: США

Когда: 29 июля 2017 год

Кто виноват: Apache Struts (Jakarta Multipart) – CVE-2017-5638

Дата выхода обновления: 7 марта 2017 года



# - 40% от стоимости акций




Published on TradingView.com, November 20, 2022 23:06:37 MSK
**EFX, 1D O:**200.00 **H:**202.49 **L:**198.73 **C:**200.04

**SolarWinds Corporation**

**SWI, 1H, SPBXM**
Volume

48.00
44.00
40.00
36.00
32.00
28.00
24.00
20.00
16.00
14.06
12.00

Июл Сен Ноя **2021** Мар Май Июл Сен Ноя

TradingView



# SolarWinds Corporation




Что: компрометация 18 000+ компаний через их ПО

Где: США

Когда: сентябрь 2019 год

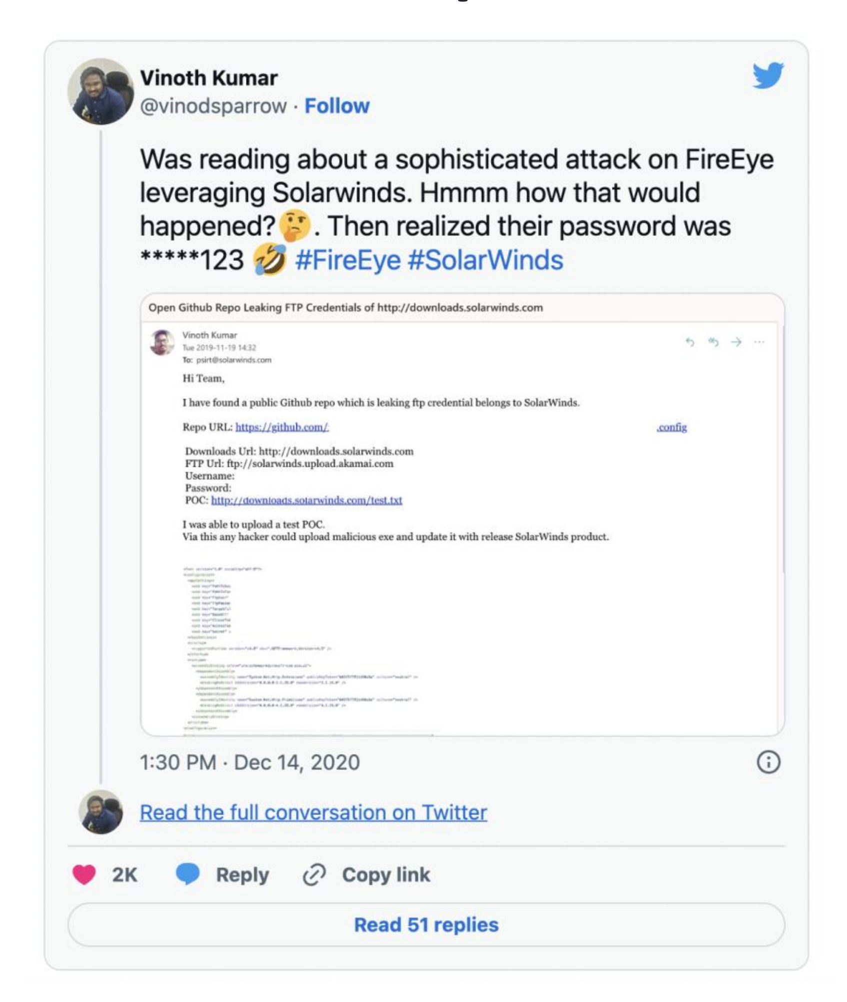
Кто виноват: внедрение вредоносного кода в сборку

Как: публичные логин и пароль в Github



# SolarWinds Corporation




*RESOLUTION*

*For SolarWinds products, to prevent possible application related issues, unexpected behaviour and performance related problems, at minimum you would need to consider excluding the following items from antivirus or security software that you install on your SolarWinds Primary, Additional, HA backup polling engines and any web servers that you run.*



# Vastaamo psychotherapy center




Что: утечка данных 30 000 клиентов

Где: Финляндия

Когда: октябрь 2020 года

Кто виноват: дефолтные учетные данные



# - 15% от стоимости акций + 10 млн $




Published on TradingView.com, November 25, 2022 07:08:29 MSK
**GRMN, 1D O:**90.2900 **H:**91.2600 **L:**90.1200 **C:**90.6200

**Garmin**



TradingView



# Garmin




Что: остановка работы сервисов

Где: США

Когда: 2020 год

Кто виноват: фишинг, непатченый сервер

Как: шифрование инфраструктуры



# Westinghouse Nuclear




Что: утечка ноу-хау

Где: США

Когда: 2017 год

Кто виноват: учетные данные в паблике, фишинг

Как: получение доступа в инфраструктуру



# Выводы




Базовая гигиена разработки



# Выводы




Базовая гигиена разработки

Не игнорировать предупреждения



# Выводы



**Базовая гигиена разработки**

**Не игнорировать предупреждения**

**Open Source — зона повышенного внимания**



# Выводы




Базовая гигиена разработки

Не игнорировать предупреждения

Open Source ⍰ зона повышенного внимания

Аккуратная публикация исходников



# Выводы




Базовая гигиена разработки

Не игнорировать предупреждения

Open Source ⍰ зона повышенного внимания

Аккуратная публикация исходников

Security ⍰ хотя бы в топ-5 приоритетов



Обратная связь
и комментарии по докладу
по ссылке



